

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Котова Лариса Анатольевна
Должность: Директор филиала
Дата подписания: 14.09.2023 15:55:03
Уникальный программный ключ:
10730ffe6b1ed036b744b6a9d97700b86e5c04a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский технологический университет «МИСиС»
Новотроицкий филиал

Аннотация рабочей программы дисциплины

Информационная безопасность

Закреплена за подразделением Кафедра математики и естествознания (Новотроицкий филиал)

Направление подготовки 09.03.03 Прикладная информатика

Профиль Прикладная информатика в технических системах

Квалификация	Бакалавр	
Форма обучения	заочная	
Общая трудоемкость	5 ЗЕТ	
Часов по учебному плану	180	Формы контроля на курсах: зачет с оценкой 4
в том числе:		
аудиторные занятия	18	
самостоятельная работа	158	
часов на контроль	4	

Распределение часов дисциплины по курсам

Курс	4		Итого	
	уп	рп		
Лекции	6	34	6	34
Практические	12	17	12	17
Итого ауд.	18	68	18	68
Контактная работа	18	68	18	68
Сам. работа	158	108	158	108
Часы на контроль	4	4	4	4
Итого	180	180	180	180

1. ЦЕЛИ ОСВОЕНИЯ

1.1	Цели освоения дисциплины: формирование у обучающихся системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.
1.2	
1.3	Задачи:
1.4	- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
1.5	- изучить основы защиты информации, а также методы, средства и инструменты шифрования, применяемых в сфере информационных технологий и бизнеса;
1.6	- получить навыки работы с методами шифрования и криптоанализа.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Блок ОП:		Б1.В.ДВ.03
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	CASE-технологии	
2.1.2	Программная инженерия	
2.1.3	Информационные системы и технологии	
2.1.4	Учебная практика по получению первичных профессиональных умений	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.2	Преддипломная практика	
2.2.3	Разработка интернет-приложений на клиентской стороне	
2.2.4	Управление IT-структурами предприятий	
2.2.5	Управление проектами	
2.2.6	Языки и среды разработки интернет-приложений	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ

ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Знать:	
ПК-2-31 информационное обеспечение и принципы построения информационных систем управления технологическими процессами	
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
Знать:	
ОПК-3-31 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	
ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Уметь:	
ПК-2-У1 использовать методы системного моделирования технологических процессов	
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
Уметь:	
ОПК-3-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	
ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Владеть:	

ПК-2-В1 современными компьютерными методами математического моделирования технологических процессов

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Владеть:

ОПК-3-В1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Введение, основы информационной безопасности							
1.1	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. /Лек/	4	8		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. /Ср/	4	20		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4			
1.3	Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. /Лаб/	4	4		Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	Раздел 2. Экономическая безопасность предприятия							

2.1	Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. /Лек/	4	8		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
2.2	Самостоятельное изучение учебного материала в LMS Canvas: Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна. Угрозы информационной безопасности. Классификация угроз. Каналы утечки информации. Модель нарушителя информационной безопасности. Классификация средств защиты информации. /Ср/	4	26		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э4			
2.3	Составление плана и основных положений политики безопасности для учреждения. /Лаб/	4	4		Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
2.4	Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Пр/	4	4		Л1.2Л2.3 Э2 Э4			
	Раздел 3. Криптографические методы защиты информации							
3.1	Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. /Лек/	4	10		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

3.2	Самостоятельное изучение учебного материала в LMS Canvas: Основные этапы развития криптологии. Основные понятия и определения. Криптостойкость. Методы криптографического преобразования данных. Кодирование. /Ср/	4	22		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
3.3	Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. /Пр/	4	4					
3.4	Шифрование текста по ключу методами замены. Шифрование текста по ключу методами перестановки. Методы шифрования текста при помощи аналитических преобразований. Шифрование текста по ключу аддитивными методами (гаммированием). Шифры с открытым ключом. Алгоритм RSA. /Лаб/	4	5		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	Раздел 4. Методы и средства защиты информации							
4.1	Методы парольной защиты. Использование простого пароля. Использование динамически изменяющегося пароля. Методы идентификации и аутентификации пользователей. Идентификация, аутентификация с помощью биометрических данных. Использование средств стеганографии для защиты файлов. Создание защищенного канала связи средствами виртуальной частной сети. Антивирусные средства защиты информации. /Лек/	4	8		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в LMS Canvas: Классификация существующих типов систем обнаружения атак (СОА). Общие понятия антивирусной защиты. Методы защиты от вредоносных программ. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	4	40		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э2 Э3 Э4			

4.3	Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. /Пр/	4	5		Л1.1Л2.1 Э2 Э4			
4.4	Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. /Пр/	4	4		Л1.1Л2.2 Э2 Э4			
4.5	Методы парольной защиты. Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому. Генератор паролей, обладающий требованиями к парольным генераторам. Диагностика антивирусной программы и создание тестовых вирусов. /Лаб/	4	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
4.6	Проведение зачета с оценкой /ЗачётСОц/	4	4		Э1 Э2 Э3 Э4			